PATENT APPLICATION
ATTORNEY DOCKET: 10624.0015

#15/C
KW3
8-15-02

In re Application of: Group Art Unit: 2131

MARCEL M. YUNG *ET AL* Examiner: H. Song

Serial No.: 09/429,624

Filed: October 29, 1999

Date: July 26, 2002

For: INCORPORATING SHARED
RANDOMNESS INTO DISTRIBUTED
CRYPTOGRAPHY

AMENDMENT

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

This response to the Office Action dated January 30, 2002 ("the Office Action") is submitted with a three-month extension fee. To place this application in better condition for allowance, please amend the application as follows.

IN THE CLAIMS:

Please amend claim 1 as follows:

C1

1. (Amended) A method of distributed cryptographic computation using a plurality of distributed electronic devices, said method comprising:

(a) computing shared values over a known and agreed context, each shared value being known by each member of a distinct subset of the plurality of distributed electronic devices;

(b) at each of a plurality of the distributed electronic devices, generating a random value using said shared values;